U.S. Department
of Transportation

United States
Coast Guard

MILITARY PERSONNEL SECURITY PROGRAM

COMDTINST M5520.12A

U.S. Department of Transportation

United States Coast Guard

Commandant
U.S. Coast Guard

2100 2nd Street SW
Washington, D.C. 20593
Staff Symbol: G-CFI
Phone: (202)267-1481

COMDTNOTE 5522
10 MARCH 1999

COMMANDANT NOTICE 5522 CANCELLED: 10 MARCH 2000

Subj: CHANGE ONE TO COMDTINST M5520.12A, MILITARY PERSONNEL SECURITY PROGRAM

1. PURPOSE. This Notice publishes changes to the Military Personnel Security Program manual, COMDTINST M5520.12A.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, Chief Counsel and special staff offices at Headquarters shall ensure compliance with the provisions of this directive.

3. SUMMARY OF CHANGES. This change publishes the Office of Security Policy and Management's new Headquarters staff symbol (G-CFI). In addition, it adds the Department of Energy "Q" clearance program to the Military Personnel Security Program. There are no significant changes to previously published policy. This change provides clarification to assist with implementation of the program.

4. PROCEDURES. Remove and insert the following pages:

Remove	Insert
Table of Contents i thru ii	Table of Contents i thru ii CH-1
Page 1-5 thru 1-10	Page 1-5 thru 1-10 CH-1
Page 2-1 thru 2-19	Page 2-1 thru 2-23 CH-1
Page 3-1 thru 3-4	Page 3-1 thru 3-4 CH-1
Enclosure (2) pages 1 thru 11	Enclosure (2) pages 1 thru 4 CH-1

Add

Record of Changes iii CH-1
Page 5-1 thru 5-3 CH-1

W. H. CAMPBELL

DISTRIBUTION – SDL No. 135

	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	3	2	3		2	2	1	2	1	1		1	2	1	1	1	1	1	1		2					
B		8	10	2	12	5	3	5	3	3	2	3	3	10	3	2	2	40	2	1	2	1	3	2	1	1
C	3	2	1	3	2	1	1	1	2	1	2	1	2	5	2	2	3	1	2	1	1	1	1	1		
D	2	1	1	3	11	1	1	1	1	1	1	1	1			1	1	1	1	1	1	1	1	1	1	1
E		2					1	1		1	1	1		1	1			1	1							
F	1	1	1	1				1		1			1		1											
G	1	1																								
H																										

NON-STANDARD DISTRIBUTION:

Director of Finance and Procurement

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE ENTERED	ENTERED BY (Printed name and signature)

TABLE OF CONTENTS

CHAPTER 1. - PERSONNEL SECURITY PROGRAM

CHAPTER 2. - MILITARY PERSONNEL SECURITY

CHAPTER ONE - PERSONNEL SECURITY PROGRAM

A. Definitions. The terms below appear throughout this Manual. They have specific meanings, some of which may differ slightly from their meanings in other contexts. Familiarity with these terms is essential to an understanding of the Coast Guard's Personnel Security and Counterintelligence Programs.

1. Access. The ability and opportunity to obtain knowledge of classified information for official duties. Access is based upon a need-to-know determination made by the holder of the classified material and access is authorized only after the issuance of a temporary, interim or final security clearance at the appropriate level.

2. Adverse action. Any action taken with respect to an individual who has been investigated under the provisions of this regulation that results in:

   a. Denial or revocation of security clearance.
   b. Denial or revocation of access to classified information.
   c. Denial or revocation of a special access authorization.
   d. Nonacceptance for or discharge from the Coast Guard when any of the foregoing actions are taken as the result of a Personnel Security determination.

3. Adjudication. An overall common sense determination based upon consideration and assessment of all available information, both favorable and unfavorable, with particular emphasis being placed on the seriousness, recency, frequency and motivation for the individual's conduct; the extent to which conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved; and, to the extent that it can be estimated, the probability that conduct will or will not continue in the future.

4. Alien. Any person not a citizen of the United States.

5. Citizen. United States citizens, either by birth or who are U. S. Nationals, those who have derived U. S. Citizenship or those who acquired it through naturalization.

6. Classified Information. Information that requires protection in the interests of National Security in accordance with Executive Order 12958.

7. Clearance. A security determination that an individual is eligible and authorized to be allowed access to classified information on a need-to-know basis. The level of clearance will not exceed the required level of access.

8. Command. For the purpose of this regulation, a Command is any organizational entity under one individual authorized to exercise direction and control. The term includes units, ships, laboratories, bases, squadrons activities, facilities or any other indication of organizational integrity.

9. Commanding Officer. Unless otherwise noted, the term "Commanding Officer" includes "Commander", "Officer-in-Charge", "Director", "Inspector" and any other title assigned to an individual, military or civilian, who through Command status, position or administrative jurisdiction, has the authority to render a decision with regard to a specific question under consideration

10. Command Security Officer (CSO). Designated by the Commanding Officer to manage the security program and to provide unit or staff level security support. Commands not required to designate a CSO per COMDTINST M5510.21 (series) shall designate a unit security officer to perform the functions designated for the CSO in this Manual.

11. Continuous Service. Continuous service refers to honorable active duty; attendance at the military academies; membership in reserve officer training corp (ROTC) Scholarship Program; Army and Air Force National Guard membership; service in the military Ready Reserve forces (including active status); civilian employment in government service, civilian employment with a Government contractor or as a consultant involving access under the DoD Industrial Security Program. Continuous service is maintained despite changes from one of the above statuses to another as long as there is no single break in service greater than 24 months.

12. Eligibility. Results from a determination made by a trained adjudicator under the standards of Enclosure (1), which establishes the highest level of final security clearance that an individual may qualify to receive. The determination will be based upon the type and recency of the member's personnel security investigation. Also, eligibility can be affected by the review of any other pertinent information relating to the member's qualification for a final security clearance.

13. Foreign National. Considered to be any person not a U.S. citizen or immigrant alien. American citizens representing foreign governments, foreign private interests, or other foreign nationals are considered to be foreign nationals for the purposes of this regulation, when acting in that capacity.

14. Immigrant Alien. Any person lawfully admitted into the United States under an immigration visa for permanent residence.

15. Interim Security Clearance. A Security Clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis,

pending the completion of the full investigative requirements. Interim clearances are valid for 180 days but may be extended if necessary.

16. Level of Security Clearance. Top Secret, Secret or Confidential and indicates the highest level of classified information to which access may be granted based on that clearance if need-to-know exists.

17. Limited Access Authorization. A certification that a person is authorized to have access only to certain specific classified information which has been carefully screened by the appropriate Security Officer for its releasability to that person.

18. National Security. The national defense and foreign relations of the United States.

19. Need-to-Know. A determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Knowledge or possession of, or access to, classified information shall not be afforded to any person solely by virtue of the individual's office, position or security clearance.

20. Personnel Security Investigation (PSI). Any investigation required for the purpose of determining the eligibility of an individual for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties or other designated duties requiring such investigation.

21. Presidential Support Activities. Coast Guard Personnel assigned to the President and Vice President as Military Social Aides, to White House communications activities and the Presidential retreat, to the Office of the Vice President, Honor Guard personnel, Ceremonial units and military bands who perform at Presidential or Vice Presidential functions and facilities and personnel in designated unites requiring a lessor degree of access to the President or Vice President are considered assigned to Presidential Support Activities.

22. Sensitive Compartmented Information (SCI). All information and materials bearing special intelligence community controls indicating restricted handling within intelligence collection programs and their end products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs.

23. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Top Secret, Secret or Confidential information. Such a program includes, but is not limited to, special clearance, adjudication, investigative requirements, material dissemination restriction, or special lists of persons determined to have a need-to-know.

24. Temporary Access. Short-term access issued to an individual at a higher level, provided all investigative requirements are met, than that to which normally assigned in order to accomplish a specific designated task.

25. U. S. National.

    a. A person born in an outlying possession of the United States on or after the date of formal acquisition of such possession or;

    b. A person born outside the United States and its outlying possessions of parents both of whom are nationals, but are not citizens of the United States, and have had residence in the United States or one of its outlying possessions prior to the birth of such person; or

    c. A person of unknown parentage found in an outlying possession of the United States while under the age of five years, unless shown, prior to attaining the age of 21 years, not to have been born in such outlying possession. For the purposes of this directive, U.S. Nationals are included in the use of the term "U.S. Citizens".

B. Basic Policies.

1. The Department of Transportation (DOT) is responsible for issuance of departmental policy for the Coast Guard to follow in the management and operation of the Military Personnel Security Program. Additionally, it directs, insofar as practicable, that operations shall be compatible with those of the DoD and DOT to facilitate the transfer of the Coast Guard to the Navy, if directed. Where possible, this Manual parallels the guidance provided by various Navy and DOT Instructions.

2. This Manual provides authority and necessary guidance for the administration of the Coast Guard Military Personnel Security and Counterintelligence Programs. It provides guidance on personnel security investigation, determinations, clearance, access to classified information, and the termination of clearances due to adverse suitability factors.

C. Applicability.

1. The personnel security policies and procedures in this Manual apply primarily to eligibility for access to classified information or assignment to sensitive duties that are subject to investigations under provisions of this Manual. This Manual is not the authority to deny or terminate military service unless loyalty is the central issue.

2. The personnel security policies and procedures for specific programs, such as the Industrial Security Program, are found in instructions governing those programs.

D. Authority and Jurisdiction.

1. The Coast Guard Military Personnel Security Program operates under the authority, provisions and guidance of DOT Order 1630.2(series), DOT Personnel Security Program.

2. Coast Guard military personnel security operations shall apply the standards and criteria of DOT Order 1630.2(series). Insofar as practicable, the operations shall be compatible with those of the DoD and DOT to facilitate Coast Guard transfer to DoD, if directed.

3. The Director, Office of Security, DOT, will periodically evaluate and report on the effectiveness of the Coast Guard Military Personnel Security Program.

4. The Office of Security Policy and Management, Commandant (G-CFI), is the program manager and administrator for the overall Security Program and serves as the President of the Personnel Security Appeals Board (PSAB

5. The Department of Department of Transportation's Transportation Administrative Service Center (TASC) security operations (hereafter referred to as the central adjudication facility (CAF)) through a memorandum of agreement, will act as the Coast Guard's central source for final Military Personnel Security Clearances. TASC has the authority to grant, revoke or deny all security clearances for military personnel.

6. Commandant (G-OCI) is responsible for the management of access to Sensitive Compartmented Information (SCI) for Coast Guard Personnel.

7. For access other than SCI, any Commanding Officer of an active duty unit may grant an interim security clearance or temporary access to any military member subject to the Commanding Officer's authority and to the relieving Officer upon the change-of-command. The Commanding Officer granting the interim clearance or temporary access shall be eligible for a security clearance equal to or higher than the interim clearance or temporary access being authorized. When it is impracticable for a departing Commanding Officer to grant an interim clearance to the relieving Officer, the interim clearance may be granted by the Executive Officer. The Command Security Officer may be designated the authority to grant interim security clearances or temporary access provided they are eligible for a security clearance at the appropriate level.

8. District Commanders or an individual designated by the District Commander, may grant interim clearance or temporary access to drilling reserve personnel not on extended active duty, under their jurisdiction.

E. Responsibilities.

1. Upon a new member arriving at a unit, Commanding Officers shall ensure that the member's need for a security clearance/access is reviewed.

2. Commanding Officers shall ensure that all personnel assigned to duties requiring access to classified information are initially indoctrinated and periodically instructed thereafter on the national security implications of their duties and their individual responsibilities.

3. Procedures shall be established, and special counseling made available in an effort to encourage individuals granted a clearance under this Manual to seek appropriate guidance and assistance on any personal problem or situation that may have a bearing on their security clearance.

4. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding a security clearance. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for a security clearance. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a security clearance rests with the individual.

F. Citizenship.

1. Only United States citizens are eligible for security clearances. Only United States citizens are eligible for assignment to sensitive duties or access to classified information unless there are compelling reasons in the furtherance of Coast Guard missions, including special expertise, to assign a non-U.S. citizen to sensitive duties or to grant a Limited Access Authorization. When this Manual refers to U.S. Citizenship, it makes no distinction between those who are U.S. citizens by birth, those who are U.S. nationals, those who have derived U.S. citizenship or those who acquire it through naturalization. "Non-U.S. citizens" are identified by this manual as immigrant aliens and foreign nationals. Immigrant aliens are those who have been lawfully admitted to the U.S. under an immigrant visa for permanent residence. Foreign nationals are those who are not U.S. citizens, U.S. nationals nor immigrant aliens to the United States.

2. Eligibility for a clearance of a person who claims both U.S. and foreign citizenship will be determined by application of the adjudication policy on dual citizenship

under “Foreign Preference” of the adjudication standards in chapter four of this Manual.

3. Under no circumstance will non-U.S. citizens be eligible for access to sensitive compartmented information, classified NATO information, COMSEC keying material, cryptologic information, intelligence information (unless authorized by the originator) or any other special access program. Enlisted non-U.S. citizens may not enter ratings which generally require access to classified information. (see COMDTINST M1000.6 (SERIES)).

4. United States citizenship must be verified prior to granting a security clearance.

G. <u>Personnel Security Data Management</u>. Personnel security records contain considerable, highly-privileged information and, in some cases, classified information. It is imperative that these records be carefully protected in their handling, transmittal, release and storage.

1. Freedom of Information Act (FOIA) or Privacy Act (PA) requests for investigative information must be addressed to the agency conducting the investigation. Release of investigative information obtained under a pledge of confidence shall be controlled in accordance with the commitment made by the investigative agency concerned. Normally this commitment would preclude divulging it to the person investigated.

2. Medical reports obtained in conduction with an investigation shall be carefully controlled to assure that the privileged, personal information is not divulged to persons who do not need it for security or suitability determination.

3. Classified investigative reports shall be protected as required by Coast Guard directives regarding control and safeguarding of classified information.

4. Records must be kept in lockable cabinets, safes or Automated Information Systems (AIS) accredited in accordance with COMDTINST M5500.13 (series), AIS Security Manual. Access must be controlled to work areas where records are maintained. Positive identification and a need-to-know is required for users of the records.

H. <u>Foreign Assignments and Foreign Travel</u>. Special safeguards are required to protect national interests and national security information when Coast Guard personnel and representatives are given foreign assignments or perform official foreign travel. For this purpose, a “foreign” location means outside the 50 States, the District of Columbia, or any of the United States possessions, territories or trust territories. Investigative requirements and security precautions specified below are applicable.

1. Investigative Requirements. Coast Guard officials designating persons for foreign assignments shall carefully screen each designee to assure that presence of the person in the foreign country is not adverse to the interests of the United States.

   a. When the assignment will not exceed 1 year, there are no special investigative requirements other than those applicable to the sensitivity and duties of the position.

   b. Coast Guard personnel assigned official travel in a foreign country must exercise good judgment at all times to assure that nothing contrary to the interests of the United States or the Coast Guard is done. Officials authorizing the travel are responsible for assuring that each traveler possesses good character and the reliability needed for the assignment. Investigative requirements for similar duties at a domestic location are applicable, except for the following:

      (1) Heads of Delegations. Any person from the Coast Guard selected to head a delegation from the United States to an international conference on other than a one-time basis must have been the subject of a single scope background investigation within the last 5 years.

      (2) Nominee as Coast Guard Representative at International Conference. Nomination to represent the Coast Guard at an international conference is subject to the completion of a NAC or a more comprehensive investigation. Normally an investigation has been conducted on Federal employees, but nomination of technical advisors from the transportation industry requires special action. At least 3 weeks prior to the national conference, the Coast Guard office arranging for the services of the industry technical advisor shall furnish to Commandant (G-CFI) the information and papers needed for processing the NAC investigation.

I. **Assignment to Presidential Support Activities**.

1. Commandant (G-CFI) is the program manager and final Coast Guard authority for assignment to Presidential Support Activities (PSA) and access to the White House.

2. The policies and procedures for evaluation of military and civilian personnel assigned to Presidential Support Activities are contained in DoD directive 5210.55 (series).

3. The adjudicative standards contained in section four of this manual will be used to ensure that only the most suitably qualified candidates are considered for nomination to Presidential support duties.

4. Presidential Support Activities are designated as Category One or Category Two. A complete listing of personnel in each category is contained in DoD directive 5210.55(series). Normally Coast Guard personnel will fall into the following categories:

   a. Category One: Military Aides to the President or Vice President

   b. Category Two: Military Social Aides, Personnel assigned to White House Communications activities and Presidential retreat, Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential or Vice Presidential functions and facilities.

5. Personnel nominated for Category One or Category Two duties must have been the subject of a single scope background investigation (SSBI) within the 36 months preceding selection. The individual's spouse or cohabitant shall be, at a minimum, the subject of a National Agency Check (NAC). If the individual marries subsequent to completion of the SSBI, the required NAC shall be conducted at that time.

6. Once the Top Secret clearance has been granted, Commandant (G-CFI) will conduct a suitability adjudication for White House Access in accordance with DOD directive 5210.55(series). If an investigation contains derogatory information that would result in denial of assignment to PSA, a letter will be sent to the member via the members Command offering the member an opportunity to explain, refute, mitigate or provide information. If necessary, a limited inquiry may be requested from Commandant (G-O-CGIS) to further investigate the derogatory information. Commandant (G-CFI) will then complete the adjudication process and make a final Coast Guard determination on behalf of the Commandant. There is no appeal associated with a final denial of eligibility determination by Commandant (G-CFI) or the White House Military Office, Security Advisor.

7. The administrative nickname "YANKEE WHITE" shall be stamped or printed in bold letters across the top of all CG-5588's pertaining to Presidential Support Activities nominees.

J. <u>Program Evaluation</u>. From time to time it is essential for commands to evaluate their individual military personnel security programs to ensure that all established procedures are complied with. Enclosure (3) to this manual will be used by commands and cognizant security managers when evaluating individual command military personnel security programs. Commands will conduct a self evaluation each year and correct any discrepancies noted. Copies of the evaluation will be submitted to the cognizant security manager.

CHAPTER TWO - MILITARY PERSONNEL SECURITY

A. General.

1. Military personnel security policies and procedures in this manual apply to eligibility for access to classified information. In order to be eligible for access to classified information an individual must meet the following criteria.

   a. Have the appropriate Personnel Security Investigation.

   b. Have been determined eligible by the Central Adjudication Facility.

   c. Be granted access by the Commanding Officer or designated official.

   d. Execute a non-disclosure agreement (SF-312).

   e. Possess a valid need to know.

B. Personnel Security Investigation.

1. A personnel security investigation (PSI) is an inquiry by an investigative agency, authorized to conduct investigations, into an individual's activities, for the specific purpose of making a personnel security determination

2. The Security Policy Board (SPB) established standard investigative guidelines which are approved by the President for use by all federal government agencies. The current investigative standards are contained in enclosure (1) of this manual. There are only three investigations which are conducted for the purposes of determining security clearance eligibility. Personnel Security Investigations are conducted by the Coast Guard Investigative Service (G-O-CGIS) as a service to the Security Policy and Management Division. These investigations are:

   a. Single Scope Background Investigation (SSBI)

   b. Single Scope Background Investigation- Periodic Reinvestigation (SSBI-PR)

   c. National Agency Check with Local Agency Check and Credit Check (NACLC)

C. Security Clearance and Eligibility Determination.

1. Once the Personnel Security Investigation is completed, it is forwarded to the Central Adjudication Facility (CAF). The CAF reviews the information in the Personnel Security Investigation and compares it to nationwide adjudication standards. These standards are contained in chapter 4 of this manual. The adjudicator will then determine whether or not the individual is eligible for a security clearance.

2. A personnel security clearance is an administrative determination that an individual is eligible for access to classified information at a specified level.

3. To be eligible for clearance and access the following requirements must be met:

   a. Top Secret: Member must have been the subject of a favorably adjudicated SSBI. If more than five years old, a periodic reinvestigation must have been requested. There can not be a break in service of more than 24 months, the member must have properly executed an SF-312 non-disclosure agreement and completion of a local records check (LRC) must be documented on CG-5588.

   b. Secret: Member must have been the subject of a favorably adjudicated NACLC (or SSBI) which is less than 10 years old. If more than 10 years old, an NACLC update must have been requested. An NACLC update is simply a new NACLC request, however a notation "NACLC update" and the reason clearance is required should be in the remarks section of the CG-5588. There can not be a break in service of more than 24 months, the member must have properly executed an SF-312 non-disclosure agreement and completion of a local records check (LRC) must be documented on CG-5588. If an individual has a favorably adjudicated NAC or ENTNAC completed prior to 1 October 1997 that is less than 10 years old it to is acceptable for up to a Secret clearance.

   c. Confidential: Member must have been the subject of a favorably adjudicated NACLC which is less than 15 years old. If more than 15 years old, an NACLC update must have been requested. There can not be a break in service of more than 24 months, the member must have properly executed an SF-312 non-disclosure agreement and completion of a local records check (LRC) must be documented on CG-5588.

D. **Access**. The ultimate authority for granting access to classified information rests with the Commanding Officer responsible for the security of the information or material at his/her command. A Commanding Officer may grant access to classified information to an individual who has an **official need to know**, a valid security clearance, has a properly executed a SF-312 on file and there is no locally available unfavorable information.

1. If significant derogatory information is discovered after the PSI and clearance determination, access will be suspended following the guidelines set forth in paragraph 2.V. of this manual. If access has not been suspended at the command level, Commandant (G-CFI) may direct that access be suspended pending resolution.

2. The number of personnel that a command grants access to classified information shall be kept to the **absolute minimum** required for the conduct of the command functions.

3. An individual's access history will be maintained at the command level for a period of four years after transfer, discharge or retirement. The Command Security Officer (CSO) will maintain a roster of all personnel assigned to their command who have been granted access to classified material. The roster will contain the following information:

   a. Name, rank and SSN

   b. Type of investigation

   c. Date investigation was completed

   d. Level of final clearance granted

   e. Expiration date for interim or temporary clearance

   f. Reason top secret access is/was required (if applicable)

   g. Date access granted/terminated

   h. Date SF 312 (non-disclosure agreement) was executed

4. Access shall not be granted solely to permit entry to, or ease of movement within, controlled areas when the individual has no need for access and access to classified information may be reasonably prevented.

5. Access will not be granted to persons who may only have inadvertent exposure to sensitive information.

6. Personnel shall not be granted access to classified information merely as a result of any particular title, rank, position, or affiliation. (Security managers with the appropriate credentials shall be authorized access in the performance of their duties).

E. Security Clearance Re-approval:

1. When an individual is transferred from a command, his/her requirement for access at that command no longer exists. Their access is therefore withdrawn even though their clearance remains unchanged.

2. Executive Order 12968 requires that all clearances are to be re-approved whenever a member with a clearance is transferred. Therefore, the member's new Commanding Officer(or a person designated in writing by the Commanding Officer) will sign a CG-5588 re-approving the individual's clearance. See exhibit 2-1 for re-approval instructions.

3. Once a clearance is re-approved, commands may grant access provided the following conditions are met:

   a. Access is only required at or below the level of clearance eligibility.

   b. The previously issued CAF source document or appropriate PMIS entries are sighted. Source documents and PMIS extracts should be on file in the individuals PDR.

   c. A thorough local records check is conducted.

   d. An SF-312 has been properly executed and a copy is on file in the member's PDR.

F. Investigative Request Procedures. Requests for personnel security investigations will be processed as follows:

1. National Agency Checks with Local Agency Checks and Credit Check. CG-5588 (1 original), SF-86 (5 copies with original signatures),a self addressed CG-4217, FD-258 (2 original), and 1 signed DOT 1631will be completely reviewed by the Command Security Officer and **forwarded to Commandant (G-O-CGIS)** to conduct the NACLCs. Commands are reminded that ENTNACS are conducted on all first term enlistees but are not valid for clearance if a clearance was not previously issued before 1 October 1997.

2. Single Scope Background Investigations. CG-5588 (1 original), SF-86(5 copies with original signatures), a self addressed CG-4217, FD-258 (2 originals), 1 signed DOT 1631, and if not included on previous

investigation; SF-86 (1 original and 1 copy with original signature, by spouse or member; completed through item 8 for subject's spouse and/or cohabitant, foreign born children over age 18, and foreign born parents.) will be forwarded to the cognizant Security Manager after complete review by the Command Security Officer. Since the number of personnel with Top Secret clearance will be kept to an absolute minimum, justification for the SSBI will be noted in the remarks section of the CG-5588 including the Billet Control Number of the subjects present billet or future billet if being transferred. The cognizant Security Manager will submit the package to Commandant (G-O-CGIS) to conduct the SSBI.

3. Scope. Some of the questions on the revised SF-86 specify a time frame of 7 years, which is not consistent with National Security Directive (NSD) 63 which requires a **10 year scope for SSBI's**, (the scope for PR-SSBI's is 10 years or to the date of the last completed SSBI) therefore, when completing SF-86 for a SSBI, the following questions will be answered with a 10 year scope. Forms received not meeting these requirements will be returned without action:

   a. Question 9, Residences

   b. Question 10, Schools

   c. Question 11, Employment Activities

   d. Question 12, References

   e. Question 21, Medical

   f. Question 22, Employment Record

   g. Question 23, Police Record

   h. Question 29 Court Actions

Note: The scope for all questions when requesting an NACLC is 7 years or to the 18th birthday, whichever is less.

4. When a security clearance is required to meet urgent operational commitments, ships that are scheduled to be underway may request message notification of clearance by indicating on the CG-5588 "message response requested".

5. The CSO will maintain a copy of the member's SF-86 until the investigation has been completed. If the member is transferred before the investigation is completed, the CSO will forward the copy to the CSO of

the receiving command. This will facilitate review by the command or subsequent commands if interim clearance is necessary.

6. Cancellation. When a personnel security investigation is in a pending status and circumstances change that negate the need for the investigation, the member's command will immediately advise their cognizant security manager and provide the reason for cancellation. The central adjudication facility (CAF) will be notified via CG-5588 only when the reason for cancellation is due to separation for cause or resignation or retirement in lieu of pending adverse action. The remarks section of the CG-5588 will provide a brief summary of the specific unfavorable information. An additional sheet is authorized if space in the remarks section is insufficient.

G. Interim Security Clearance. An interim security clearance is granted temporarily, pending completion of full investigative requirements. Interim clearances are granted by authority of the Commanding Officer and will be recorded on the CG-5588 (see paragraph 2-L). Prior to granting interim clearance, commands shall ensure that the member has a properly executed SF-312 on file.

1. Interim Confidential/Secret:

   a. Conduct a local records check of unit Personnel Data Record (PDR), medical record and any locally maintained training files.

   b. Review the member's completed Questionnaire for National Security Positions (SF-86), ensure that all information required is provided and complete. If unfavorable information is contained in the SF-86, interim clearance may not be granted without adjudication of the completed investigation by the central adjudication facility (CAF).

   c. If the local records check and the SF-86 contain no unfavorable information, the interim clearance may be granted

   d. The interim clearance is valid for a period not to exceed 270 days.

2. Interim Top Secret:

   a. Conduct a LRC of unit personnel data records, medical records and any locally maintained training files.

   b. Review the member's completed Questionnaire for National Security Positions (SF-86), ensure that all information required is provided and complete. If unfavorable information is contained in

the SF-86, an interim clearance will not be granted without adjudication of the investigation by the CAF.

c. Review the Questionnaire for National Security Positions (SF-86) completed for spouse and/or cohabitant and foreign-born parents and/or children over age 18.

d. Review the Personnel Management Information System (PMIS) or equivalent and ensure that a favorable personnel security investigation of any type has been completed within the last 20 years

e. If the LRC and the SF-86 result in favorable review and the prior investigation was adjudicated favorably with no break in service exceeding 24 months since the investigation was completed, an Interim clearance may be granted.

f. Forward the investigation package to the cognizant Security Manager, ensuring that thorough justification for an SSBI is in the remarks section of the CG-5588. The cognizant Security Manager will review the package for correctness, certify the justification and submit the package to Commandant (G-O-CGIS).

g. The Interim Top Secret clearance is valid for a period not to exceed 365 days.

h. If the LRC and the SF-86 result in favorable review, and, after contacting the cognizant security manager a prior investigation cannot be confirmed or does not exist, Commandant (G-CFI) must grant the interim clearance. Submit a message action to Commandant (G-CFI), information to the cognizant security manager, containing the following information:

(1) Member's name/rate/rank

(2) Member's SSN

(3) Member's date and place of birth

(4) Name of person conducting *favorable* review of LRC and SF-86

(5) Date SSBI package submitted to cognizant security manager.

(6) Reason interim Top Secret clearance is necessary

H. **Extension of Interim Security Clearance**. If a final personnel security clearance is not received and no unfavorable information has been developed locally, the Commanding Officer may extend the interim security clearance. This extension process may continue until final determination has been received from the central adjudication facility (CAF). Note the extension on the original CG-5588 used to grant the interim clearance. The cognizant security manager will be notified of any interim clearance which has been in effect for more than 12 months.

I. **Granting Interim Security Clearance When the SF-86 Cannot Be Reviewed.** If a member granted an interim security clearance is transferred prior to the completion of the full investigative requirements, the receiving command may utilize the previous commands interim decision to grant an interim clearance, provided no new derogatory information is uncovered in the local records check. Commands should note on the CG-5588 that the SF-86 was not reviewed and the interim clearance was granted based on the previous commands review of the SF-86. Both CG-5588's should be maintained until the investigation is completed and a final clearance eligibility is made by the CAF.

J. **Clearance Based on an Investigation From Another Agency**.

1. If there is no current Coast Guard investigation on file, but the command has evidence that an investigation was conducted by an other agency, that investigation may be used as a basis for granting clearance if the investigation is within scope, was favorably adjudicated, provides the same coverage as the Coast Guard investigation and there was no break in service over 24 months since the investigation was completed. Submit a CG-5588 and annotate the type of investigation and the agency which conducted it in the remarks block. Attach any source document or certificate of clearance from the other agency if available and submit to Commandant (G-CFI).

2. If the prerequisite investigative requirements cannot be obtained, then a new investigative request for the appropriate clearance level must be forwarded to the Commandant (G-O-CGIS) (via the cognizant Security Manager if an SSBI or SSBI (PR) are requested). The requesting command may issue an interim clearance to meet the unit's operational needs, following the Interim Security Clearance procedures in this Manual.

K. **Coast Guard Personnel Assigned to Other Components**. Coast Guard personnel assigned to another service often require a security clearance. Commandant (G-CFI) will ensure that the appropriate security clearance determination is made and the other activity is notified accordingly. If an investigation is required, all investigative paperwork will be completed by the member and submitted to the cognizant security manager for review and submission to Commandant (G-O-CGIS).

L. Clearance Notification When Visiting Another Command.

1. When a Coast Guard member is visiting another command (Coast Guard or other) notification of the member's clearance level may be required.

2. An official letter from the member's command to the command being visited will be sent and must indicate the following:

   a. Member's name (last, first, middle).

   b. Member's rank/rate.

   c. Member's SSN (last 4 digits).

   d. Member's clearance level (final/interim).

   e. Basis of clearance (NAC, SSBI) and date completed.

   f. Date member executed the SF-312.

3. In cases where time will not allow an official letter to be received, message/fax notification may be made provided it contains the above information.

4. Hand carried clearance information is not authorized.

M. Coast Guard Form 5588.

1. A CG-5588 will be used to request security clearances, re-approve a clearance, grant an interim clearance, document that an interim security clearance is extended, for follow-up and tracer actions, to report derogatory information or status change (i.e., upgrades and downgrades of access). Exhibit 2-2 shows an example of a CG-5588.

2. To ensure uniform submission of information and timely response, other locally produced forms or letters will not be accepted. It is vital that all requested information on the CG-5588 be completed. Incorrect or incomplete forms will result in delay of action as the forms will be returned to the originator for resubmission.

3. As this form is used for a number of different actions, the following is a guideline for proper completion:

   a. Clearance re-approval. Complete items 1 thru 8, 12 thru 15, 18 and 26.

b. Interim clearance. Complete items 1 thru 8, 12 thru 15, 16 or 17 (as appropriate) and 26.

c. Granting access. Complete items 1 thru 8, 12 thru 15, 18 and 26.

d. Requesting PSI and clearance determination. Complete items 1 thru 8 (1 thru 11 if the request is for SCI)12 thru 15, 20 thru 21 and 24 thru 26.

e. Reporting derogatory information. Complete items 1 thru 8, 24 and 26. (note type of report i.e. Initial, interim or final and provide details in block 24).

f. Interim clearance extensions. Note "interim clearance extended until (date)" and initial in item 24 of the CG-5588 originally granting the interim clearance.

N. Central Adjudication Facility Procedures.

1. Commandant (G-CFI) forwards all completed investigations to the central adjudication facility (CAF) for adjudicative action. The central adjudication facility (CAF) will make personnel security determinations based on the highest eligibility the investigation will support and grant the clearance identified on the CG-5588.

2. The central adjudication facility (CAF) will make clearance notifications via PMIS updates and a certificate of clearance issued to the requesting command.

3. Reserve Personnel. Coast Guard Reserve Personnel in an active status may be issued security clearances when necessary. The clearance will be requested by the unit where the individual is administratively assigned. All investigative and documentation procedures remain the same as for active duty personnel.

O. Administrative Procedures.

1. Certificate of Clearance. When the central adjudication facility (CAF) makes a favorable security determination, notification is made via PMIS updates and a certificate of clearance known as the source document. This source document shall have a properly executed SF-312 and CG-5588 attached and be filed in the members PDR.

2. Periodic Reinvestigation and Investigation Updates. An investigation must be updated from time to time as part of the continuous evaluation program, for those personnel who require access to classified information. The time periods for periodic reinvestigations and investigation updates depend upon the level of clearance. Time periods are contained in para 2.C.3. of this manual. The requirement to conduct a periodic reinvestigation or an investigation update does not have an effect on an initial clearance determination unless the member has a break in service of over 24 months or the eligibility is revoked by the CAF. It is not necessary to lower clearance or grant an interim clearance just because the investigation may be past the required update or reinvestigation date unless the member fails to submit the required paperwork for the reinvestigation or update within 30 days of the clearance re-approval.

3. Clearance/Access Briefing. Each person who is granted access to classified information will be given a Clearance/Access brief prior to granting the actual access. The briefing shall be conducted per chapter three of this manual.

4. Investigations Update. The Command Security Officer will review the monthly PMIS/JUMPS control report to ensure that updated investigations are requested in a timely manner on all personnel who still require access to classified information.

5. Transfer Briefings. When individuals are transferred they must be given a transfer briefing per chapter three of this manual. This briefing is required regardless of whether or not the individual had access at the command as the individual may have had inadvertent access to sensitive information.

6. Final Termination Briefing. All personnel departing Coast Guard service, or personnel who's clearance is revoked by the CAF, will be given a final termination briefing per chapter three of this manual. This briefing is required regardless of whether or not the individual had access at the command as the individual may have had inadvertent access to sensitive information. Final termination briefings are documented by completing the Security Debriefing Acknowledgement section of the SF-312 and forwarding the completed form to Commandant (CGPC-ADM-3).

7. Disposition of old Personnel Security Record (CG-5274).

   a. The CG-5274, Personnel Security Record is obsolete.

   b. All CG-5274's will be forwarded to Commandant (CGPC-adm3) for inclusion in the members permanent record. Ensure all previous

source documents and SF-312 copies are removed and retained in the individuals PDR.

P. <u>Unfavorable Personnel Security Determinations</u>.

1. When the central adjudication facility (CAF) makes an unfavorable personnel security determination, action to deny or revoke security clearance or eligibility is initiated, a Letter of Intent (LOI) listing the disqualifying factors will be forwarded to the subject via their Commanding Officer, with copies to Commandant (G-CFI) and the cognizant Security Manager. The Command Security Officer shall notify the cognizant Special Security Officer (SSO) of the LOI if SCI access is involved. A form letter acknowledging receipt of the LOI will also be enclosed. <u>Commands shall ensure that the acknowledgment is signed by the member and forwarded to the central adjudication facility (CAF) with a copy to Commandant (G-CFI) and the cognizant security manager</u>. When the acknowledgement is received, the central adjudication facility (CAF) will make a final determination and advise the individual via the Commanding Officer and Commandant (G-CFI). If the final decision is favorable, a copy of the notification will be forwarded to Commandant (G-CFI) and the cognizant Security Manager. If the final decision results in a denial or revocation, the subject will be advised of his/her rights by letter from the central adjudication facility (CAF) via Commandant (G-CFI) and the Commanding Officer. A copy will be forwarded to the cognizant Security Manager. The central adjudication facility (CAF) will forward all pertinent paperwork to Commandant (G-CFI) for insertion into the members security file.

2. <u>Appeal to Denial or Revocation Action</u>. In order to appeal an unfavorable decision issued by the central adjudication facility (CAF) Coast Guard personnel must first file an appeal with the Coast Guard Personnel Security Appeals Board (PSAB). The PSAB is established under the authority of the Commandant and is the sole Coast Guard appellate authority for unfavorable personnel security determination appeals by Coast Guard personnel. If the PSAB decision is adverse, the individual may appeal the decision to the Department of Transportation Personnel Security Review Board (PSRB) for a final decision.

   a. <u>Effect of failure to appeal</u>. Failure of an individual to submit an appeal within the prescribed time allotted to the PSAB or an indication of an intent not to appeal will result in the security determination becoming a final decision. If a member declines appeal they shall be counseled by the command on the effect of this decision on their future eligibility to remain in or apply for ratings or assignment requiring a security clearance.

b. Requests for extensions to file an appeal will be granted only for good cause and must have a command endorsement. Submission of a request for an extension does not automatically authorize a delay in the filing of an appeal beyond the normal time limits. Appeals postmarked more than 30 calendar days after the date the individual signed the notification of a final security determination notification will be rejected as untimely. The appellant will be notified of the decision on his/her request for an extension via their Commanding Officer.

c. Commandant (G-CFI) will appoint no less than six military officers, 0-4 or above, to serve as members of the PSAB when selected.

d. The PSAB will be comprised of three members. The Coast Guard Director of Security , Commandant (G-CFI) will serve as the President and will select appointed officers to serve on each PSAB as necessary.

e. Commandant (G-CFI) will provide an executive secretary for the PSAB to administer operations of the board.

f. When an appeal is received Commandant (G-CFI) will:

(1) Govern the frequency of the meetings to review appeals;

(2) Set places and times of the meetings;

(3) Determine review procedures to be followed; and

(4) Handle all administrative matters.

g. The PSAB will adhere to the following procedures:

(1) Upon receipt of an appeal, the secretary will retrieve the investigations and/or other security files and notify members of the PSAB.

(2) The PSAB will review the appeal correspondence and associated case files pursuant to the adjudication guidelines contained in chapter four of this Manual. The PSAB decision will be based solely on the written record including any writings submitted by the member. The member is entitled to a personal appearance before the PSAB to answer questions and submit any additional pertinent information. The member will be notified in writing by the

board if during an initial meeting the board does not intend to overturn the central adjudication facility (CAF) decision. The personnel appearance will be arranged and funded by the individual's command.

(3) The President of the PSAB will sign and forward the final appeal decision to the appellant via his/her Commanding Officer with copies to the central adjudication facility (CAF). The appellant can appeal the PSAB decision to the Department of Transportation Personnel Security Review Board (PSRB). Commandant (G-CFI) will retain the completed appeal file.

3. Reconsideration. Coast Guard military members whose security clearance or eligibility have been denied or revoked are not eligible for reconsideration by the PSAB for 1 year from the date of the central adjudication facility (CAF) denial or revocation. Commanding Officers may request reconsideration by providing a CG-5588 request to the central adjudication facility (CAF) via Commandant (G-CFI), together with their rationale as to why the denial or revocation should be reconsidered.

Q. Investigations Affecting Suitability for Coast Guard Service.

1. When a personnel security investigation reveals information that would affect a member's suitability for Coast Guard service, Commandant (G-CFI) will forward the investigation to Commandant (G-CGPC-epm or opm) for a final retention determination. If a favorable retention decision is made and a security clearance is required, the investigation will be returned to Commandant (G-CFI) to facilitate the security clearance determination.

2. The factors listed below may be considered as a basis for determining if a member is unsuitable for Coast Guard service:

a. Misconduct or negligence in prior assignments that would have a bering on efficient service, or would interfere with or prevent effective accomplishment of Coast Guard missions and responsibilities;

b. Criminal conduct or dishonest conduct, which may have an impact on the members ability to perform his/her duties and responsibilities;

c. Intentional fales statement, deception, or fraud;

d. Alcohol abuse of a nature and duration which suggests that the member would be prevented from performing his/her duties and responsibilities;

e. Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;

f. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; or,

g. Refusal to furnish testimony during an investigation, inquiry, or personnel security interview.

R. **Requests for Additional Information**. The central adjudication facility (CAF) is authorized to request additional pertinent information, forms or evaluation to resolve issues. Commanding Officers shall provide responses to those requests in a timely manner in order to facilitate processing. Each request will contain a suspense date for response. The central adjudication facility (CAF) shall be advised of any delays past that suspense date. Additional time to respond will be given when possible.

S. **Single Scope Background Investigations for Sensitive Compartmented Information**.

1. In order to grant access to SCI, military personnel are first required to possess a Top Secret clearance. As such, current SSBI is necessary. When required, military personnel should follow the procedures previously described in this chapter in filling out the SF-86. Prior to actual submission of the forms, candidates for SCI access will be subject to a pre-nomination interview to determine their suitability for further processing for SCI access. The pre-nomination interview will be conducted by the Special Security Officer (SSO) if available or as directed by the cognizant security manager.

2. The CG-5588 will be filled out as previously noted with the following additions:

a. Block 18: Check the box marked SCI and note authority (provided by the SSO).

b. Block 20: Check the box marked SSBI, and

c. Block 21: Check the Top Secret box and the SCI box.

3. To request SCI access for personnel who hold a current SSBI and Top Secret eligibility, the SSO should submit a CG-5588 and the completed pre-nomination interview to Commandant (G-OCI).

4. Any changes in personal status involving a current marriage, either intention to or actual marriage to a foreign national, proposed name change, or changes in cohabitation shall be reported to the appropriate SSO. The member should provide the SSO an SF-86 on the spouse/cohabitant, (items 1-8, 13, member may sign for spouse). The SSO will prepare a CG-5588 and shall annotate block 23 with "change in marital status/cohabitant status". The SSO will then forward a copy of the CG-5588 to Commandant G-O-CGIS.

T. **Administrative Withdrawal of Access**.

1. If an SSBI/PR is in progress at the time of the 5 year anniversary of the SSBI, the Top Secret clearance will not be administratively adjusted. However, if the Top Secret clearance is held based on a SSBI that is older than 5 years and the individual fails to provide paperwork for a periodic reinvestigation within 30 days, the Commanding Officer will remove access and notify the cognizant security manager.

2. When a Secret clearance is held based on an investigation that is older than 10 years and the individual fails to provide paperwork for a periodic reinvestigation within 30 days, the Commanding Officer will remove access and notify the cognizant security manager.

3. Commanding Officers will administratively withdraw an individual's access if the individual refuses to submit any required investigative paperwork.

4. A waiver to the above requirements maybe be requested in writing from the cognizant security manager.

U. **Temporary Access**. Coast Guard military personnel may be granted temporary access if the individual is determined to be otherwise eligible for the access involved, but does not currently hold a security clearance at that level. Temporary access to SCI material, although not typically justified, falls under the purview of Commandant (G-OCI). Situations in which temporary access may be justified include attendance at a classified meeting or training session, participation in advancement examinations or annual reserve active duty for training. If temporary access is justified, the Commanding Officer may, after favorable review of locally available records, allow access or certify to another command the individual's eligibility for access. This provision is made to relieve commands and the central adjudication facility (CAF) of the administrative burden of taking normal action to temporarily reissue or raise an individual's security clearance temporarily. It does not apply when an individual's assigned duties require continued access, even

intermittently. Temporary access is limited to 30 days, and will be granted no more than twice per year to any one individual and may not be granted under any circumstances to individuals whose security clearance, eligibility or access has been denied or revoked. When access is granted a CG-5588 will be completed citing this paragraph in the remarks section and will indicate the level of temporary access and the dates authorized. CG-5588's for temporary access will be maintained by the command for a period of four years after the temporary access is removed.

V. **Continuous Evaluation of Eligibility**.

1. Derogatory Information.

   a. Each member's eligibility for access to classified information shall be continuously evaluated. Commanding Officers shall report all derogatory information on personnel holding security clearance eligibility to Commandant (G-CFI) via CG-5588 with an information copy to the cognizant Security Manager, (information involving civil arrest or conviction will also be sent to CGPC-OPM/EPM and ADM-3) as soon as the incident occurs. The CG-5588 will cite the incident and the date it occurred, if access has been suspended and final disposition (if known). If the incident is pending a final disposition, the remarks section should be clearly marked "INITIAL REPORT". Documentation shall be attached as an enclosure on all reports.

   b. If an initial report is sent, Commandant (G-CFI) will hold any adjudicative action in abeyance for 60 days or until a final report is received. If the investigation, inquiry or disposition is still pending at the end of 60 days, forward a CG-5588 to Commandant (G-CFI) marked "INTERIM REPORT" and provide the progress. Interim reports shall be submitted every 60 days until the investigation, inquiry or disposition is finalized. The final results shall be forwarded to Commandant (G-CFI) via CG-5588 marked as "FINAL REPORT" in the remarks section.

   c. The decision as to whether or not to report information is not based on the individual's performance at their current command. Since commands do not have access to investigative files they cannot determine what previous adjudicative issues may be present. It is therefore essential that all derogatory information outlined in para d. below received on personnel having a security clearance eligibility be reported immediately.

d. Derogatory information which is found in the following personnel security factors will be immediately reported to Commandant (G-CFI) including any action taken by the command:

(1) Illegal use or abuse of drugs or alcohol

(2) Theft or dishonesty

(3) Lack of reliability, irresponsibility, immaturity, instability or recklessness.

(4) The use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

(5) Moral turpitude, sexual promiscuity, heterosexual promiscuity, aberrant, deviate or bizarre sexual conduct or behavior, transvestism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, spouse-swapping, window peeping and similar situations from whatever source.

(6) Records or testimony of military service where the individual was involved in serious offenses or incidents what would reflect adversely on the honesty, reliability, trustworthiness or stability of the individual.

(7) Mental, nervous, emotional psychological, psychiatric or character disorders/behavior or treatment reported or alleged from any source.

(8) Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy or evidence of living beyond the individual's means.

(9) Any other significant information relating to the criteria included in chapter four of this manual.

2. When the individual has clearance eligibility, repeated minor infractions or infractions serious enough to cause a member to be processed under the Uniform Code of Military Justice (UCMJ), will be reported.

3. Relationship With Foreign National. Any Coast Guard military member who marries or cohabits with a foreign-born, non-U.S. citizen must inform his or her Commanding Officer, must complete an SF-86 on the spouse/cohabitant and must forward the form to Commandant (G-O-

CGIS) within 30 days of the marriage/cohabitation. This must be done regardless of whether the military member is eligible for or possesses a security clearance. All members shall be cautioned that marriage or cohabitation with a foreign-born, non-U.S. citizen may result in the loss of eligibility for a security clearance. The requirements of this subsection are in addition to any other requirements of directives, publications, laws or regulations which may apply.

W. **Suspension of Access**. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the Commanding Officer may limit or suspend access. Once access is suspended or limited, it can only be restored by a CAF determination or approval from Commandant (G-CFI). Commands are encouraged to consult with their cognizant security manager prior to suspension or limitation of access. Once access is suspended or limited the cognizant Security Manager shall be notified immediately. The Commanding Officer shall forward **all pertinent information** concerning the individual to Commandant (G-CFI) for a clearance eligibility determination via CG form 5588 completing items 1 thru 8, 24 and 26 and note "initial, interim or final report of derogatory information" in block 22. Permanent change of station orders which may already be in effect on the individual must be canceled or held in abeyance and proper notification made to Commandant (CGPC).

X. **Tracer Actions**. **Tracer actions will not be submitted if the member has been granted an interim clearance**. If an interim clearance cannot be granted, tracer requests may be sent to Commandant (G-CFI) via CG form 5588 completing items 1 thru 8 and 24 thru 26 noting "TRACER REQUEST, NACLC, SSBI OR PR-SSBI (as appropriate) SUBMITTED YYMMDD" in the remarks section.

Y. **Security Clearances and Access for non-United States Citizens**.

1. The authority to grant clearance or access to non-U.S. citizens has not been delegated to the Coast Guard. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that require access to classified information. However, when it is determined that employment of a non-U.S. citizen in duties requiring access to certain classified information relating to a specific program is necessary in furthering the mission of the Coast Guard and when such access is clearly consistent with the interests of national security, a clearance or limited access authorization may be requested from the office of the Secretary by Commandant (G-CFI), upon request to Commandant (G-CFI) from the command in accordance with the procedures outlined below.

2. Non-immigrant aliens are not eligible for any level of security clearance, but may be processed for Limited Access Authorization when circumstances justify.

3. Immigrant Aliens

a. When an immigrant alien requires access to classified material (Secret or confidential only) consideration should be given to requesting issuance of a Limited Access Authorization by letter to Commandant (G-CFI). If this is impracticable, the command proposing such access shall submit a letter request for processing of a security clearance to Commandant (G-CFI). Either request must explain the reasons why the clearance is needed, identify the specific duties that require access to classified information and the nature of the material to which access is required.

b. The requesting command must ascertain that the individual has valid immigrant alien status and include a statement to that effect on the request. Such status may be determined by sighting the Alien Registration Receipt card (INS Form I-151 or I-551), issued by the Immigration and Naturalization Service. Any member not having such a card must be considered as a non-immigrant alien.

(1) The I-151 is a laminated, billfold sized blue or green card bearing the person's photograph, name, date of birth and alien registration number, and date and port of entry symbol.

(2) The I-551 is a newer card of similar size that is laminated and bears the person's photograph, name, date of birth and alien registration number. The reverse of the card contains numerical data that is only decipherable by the USINS except for the alien registration number that appears in the block in the upper left and which should correspond to the number on the front of the card.

c. The letter request shall be accompanied by a request for a SSBI, if such an investigation has not already been conducted on the individual.

d. Commandant (G-CFI) will review the letter request and forward it to the Office of the Secretary for consideration. The Director, Office of Security (Office of the Secretary) may issue an Interim Secret or Confidential clearance to an immigrant alien based upon the completion of a favorable National Agency Check pending the completion of an SSBI. When the SSBI is completed, the Director has the discretion to issue the final clearance or, a Limited Access Authorization in lieu of a security clearance.

e. When an individual is admitted to the U.S. for permanent residence, a presumption is established that there has been a change of national allegiance from the native country to that of the U.S. When an individual becomes eligible for citizenship, but elects not to be a citizen, the presumption of primary national allegiance to the U.S. is placed in doubt. Accordingly, if an immigrant alien does not become a U.S. citizen within 12 months after becoming eligible for citizenship, any personnel security clearance shall be administratively reviewed to determine if it is clearly consistent with the national security to continue the clearance. Non-U.S. citizens currently holding clearances who are eligible for U.S. citizenship may continue to have the clearance for a period of 12 months after which their status will be reviewed to determine continuing need in accordance with this Manual.

f. When a security clearance or Limited Access Authorization is received, access may be granted as necessary.

g. Immigrant aliens will not be granted access to Top Secret material.

Exhibit 2-1

Exhibit 2-2

CHAPTER THREE - COUNTERINTELLIGENCE AND SECURITY AWARENESS

A. Briefings.

1. Each Coast Guard member must be given briefings from time to time in order to ensure that they understand his/her responsibility in regards to classified and sensitive material/information.

2. The Security Awareness, Training and Education (SATE) Program COMDTINST M5528.1(series), contains example briefings which may be used to develop a briefing that will meet the specific needs of the command.

3. The Command Security Officer is responsible for ensuring security briefings are properly conducted and documented. The Command Security Officer may delegate other individuals to conduct the briefings; however, the ultimate responsibility rests with the Command Security Officer.

4. The briefings listed below represent the minimum requirements:

   a. Arrival Briefing. All personnel reporting aboard a Coast Guard unit will be given an arrival briefing. The briefing will make the individual aware of appropriate security personnel at the unit, their responsibilities and how to contact them. The briefing will also ensure that the individual is able to identify classified material and is knowledgeable of actions to be taken if classified material is discovered unattended. The briefing should identify any unit specific Operations Security (OPSEC) threats or concerns.

   b. Access Briefing. Personnel who have been determined to require access to classified information will be given an access briefing. This briefing will be conducted prior to actual access to any classified information. The briefing will insure that the individual is aware of his/her responsibility in protecting classified information, unauthorized disclosure, and compromise reporting procedures.

   c. SF-312 Nondisclosure agreement.

      (1) All Coast Guard personnel who will be granted a clearance for access to classified information must be briefed and execute a SF-312 nondisclosure agreement.

      (2) This briefing and agreement need only be executed once in an individuals career provided it is executed correctly and certified copies are locally available.

(3) Commanding Officers will ensure personnel receive the briefing required in the terms of the SF 312 and have the opportunity to read the sections of titles 18 and 50 of the United States Code and other acts referred to in the agreement.

(4) Subsequent to its execution, the SF-312 must be accepted on behalf of the United States. The accepting official can be the Commanding Officer, the Executive Officer or the Command Security Officer.

(5) If an individual refuses to sign a SF 312, the command will deny him/her access to classified information, terminate any current access immediately and inform Commandant (G-CFI) via CG-5588 with a copy to the cognizant security manager.

(6) Original SF-312's will be sent to Commandant (CGPC-ADM-3) with copies in the members PDR. Commandant (CGPC-ADM-3) will retain SF-312's as part of the member's permanent record. Improperly executed SF-312's will be returned to the unit with a copy to the cognizant Security Manager.

d. Foreign Travel Briefing. All personnel traveling to a foreign country must be given a foreign travel briefing whether the travel is official or in a leave situation. The briefing will inform personnel of general safety precautions and any information specific to the country being visited. After the travel is conducted, a debrief will be conducted to provide individual(s) the opportunity to report any incident - no matter how insignificant it might have seemed, that could have security implications. Any suspicious incidents shall be reported to the cognizant Security Manager IAW the provisions of this chapter.

e. Refresher Briefings. Once a year, all personnel who have access to classified information will receive a refresher briefing. Refresher briefings will be conducted by direction of the Command Security Officer but may be given by supervisory personnel. Refresher briefings are designed to enhance security awareness and may be given to all assigned personnel in the form of a command security stand down. The refresher brief should touch on general security matters and any recent changes in policies or procedures.

f. Final Termination Briefing. Personnel shall be given a termination briefing upon termination of government service, or when a clearance is revoked for cause. The briefing shall remind personnel to return all classified material in their possession, and they remain subject to the provisions of the criminal code and other applicable laws relating to the unauthorized disclosure of classified information. The SF-312 will be utilized to conduct this briefing and sent to Commandant (CGPC-ADM-3) for inclusion in the members permanent record.

B. Documentation of Briefings.

1. Commands will develop their own briefings based on the minimum requirements above. A record of individuals briefed will be attached and maintained for a period of four years after the latest action. The record will contain names of individuals receiving and conducting the brief, the date conducted and signatures of both. If unit level briefings are conducted a roster may be attached rather than individual entries. Each new briefing must have its own record in order to ensure that there is documentation not only of who was briefed, but what the brief consisted of. Whenever a brief is changed or altered, a new record of briefing is required.

A. Counterintelligence.

1. General.

   a. Counterintelligence refers to those activities, which are devoted to discovering, neutralizing, or destroying the effectiveness of foreign intelligence activities and to the protection of individuals against subversion, and installations or material against sabotage.

   b. In the performance of its missions the Coast Guard interacts with other countries in the areas of law enforcement, military exchanges and port visits. This interaction may subject Coast Guard personnel to foreign intelligence collection efforts. These intelligence efforts may continue regardless of shifts in governments and policies of states. These facts dictate that the Coast Guard have a policy to protect its personnel and information from foreign intelligence collection efforts.

   c. All Coast Guard personnel, whether they have access to classified information or not, shall report to their CSO any activities described in this chapter involving themselves or others. Commanding Officers will, in turn, notify the cognizant Security Manager in accordance with the procedures set forth in this chapter.

   d. Coast Guard personnel who have access to classified information shall be aware of the techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

2. Sabotage Espionage or Deliberate Compromise.

   a. Individuals becoming aware of possible acts of sabotage, espionage, deliberate compromise or other subversive activities shall report all available information concerning such action immediately to their CSO. The Command receiving

the report shall notify the cognizant Security Manager. If the cognizant Security Manager cannot be contacted immediately and the report concerns sabotage, indicates that there is a serious threat to the security of classified information through espionage, or immediate flight or defection of an individual, the unit shall send an immediate message classified at the level of the threatened information action to Commandant (G-CFI) with an information copy to the cognizant Security Manager.

b. The cognizant Security Manager shall be notified immediately of any requests, through other than official channels, for classified national security information from anyone regardless of nationality, or for unclassified information from any individual believed to be in contact with a foreign intelligence service. Examples of requests to be reported include attempts to obtain: names, duties, personal data or characterizations of Coast Guard personnel; technical orders, manuals, regulations, base directories, personnel rosters or unit manning tables; and information about the designation, strength, mission, combat posture, and development of ships, aircraft and weapons systems.

c. The Security Manager will advise the unit of what additional action, if any will be taken. The Security Manager will then notify Commandant (G-CFI) who will effect liaison and coordination with pertinent members of the U.S. intelligence community.

3. Suicides or Attempted Suicides. When an individual with access to classified information commits or attempts to commit suicide, immediately report all available information to the cognizant Security Manager with an information copy to Commandant (G-CFI). The report should set forth the nature and extent of classified material to which the individual had access and the circumstances surrounding the incident. Classified material signed out to the individual will be immediately inventoried and accountability records reconciled. Combinations to all classified containers to which the person had access will be changed immediately. Discrepancies in classified holdings will be immediately reported as a possible compromise per the Information Security Program Manual, COMDTINST M5510.21(series).

4. Unauthorized Absence. When an individual (Military or Civilian) who has had access to classified material is absent without leave (AWOL), the individual's Commanding officer will attempt to determine if there are any indications that the person may place or attempt to place themselves under the control of a foreign nation or that their activities, behavior or associations may threaten national security. In those cases where there are such indications, the Commanding Officer shall immediately forward all available information to the cognizant Security Manager with an information copy to Commandant (G-CFI).

CHAPTER FOUR- ADJUDICATIVE GUIDELINES

A. PURPOSE. The following adjudicative guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations.

B. ADJUDICATIVE PROCESS

1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

    a. The nature, extent, and seriousness of the conduct
    b. The circumstances surrounding the conduct, to include knowledgeable participation
    c. The frequency and recency of the conduct
    d. The individual's age and maturity at the time of the conduct
    e. The voluntariness of participation
    f. The presence or absence of rehabilitation and other pertinent behavioral changes
    g. The motivation for the conduct
    h. The potential for pressure, coercion, exploitation, or duress
    i. The likelihood of continuation or recurrence

2. Each case must be judged on its own merits and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security and considered final.

3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following:

a. Allegiance to the United States
b. Foreign influence
c. Foreign preference
d. Sexual behavior
e. Personal conduct
f. Financial considerations
g. Alcohol consumption
h. Drug involvement
i. Emotional, mental, and personality disorders
j. Criminal conduct
k. Security violations
l. Outside activities
m. Misuse of Information Technology Systems
n. Each of the foregoing should be evaluated in the context of the whole person.

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior.

5. However, notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

6. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

    a. voluntarily reported the information;
    b. sought assistance and followed professional guidance, where appropriate;
    c. resolved or appears likely to favorably resolve the security concern;
    d. has demonstrated positive changes in behavior and employment;
    e. should have his or her access temporarily suspended pending final adjudication of the information.

7. If after evaluating information of a security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

8. The information in bold print at the beginning of each adjudicative guideline provides a brief explanation of its relevance in determining whether it is clearly consistent with the interest of national security to grant or continue a person's eligibility for access to classified information.

C. ALCOHOL CONSUMPTION

1. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

2. Conditions that could raise a security concern and may be disqualifying include:

    a. alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;
    b. alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;
    c. diagnosis by a credentialed medical professional* of alcohol abuse or alcohol dependence;
    d. habitual or binge consumption of alcohol to the point of impaired judgment;
    e. consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program

3. Conditions that could mitigate security concerns include:

    a. the alcohol related incidents do not indicate a pattern;
    b. the problem occurred a number of years ago and there is no indication of a recent problem;
    c. positive changes in behavior supportive of sobriety;
    d. following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional.

D. ALLEGIANCE TO THE UNITED STATES.

1. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

2. Conditions that could raise a security concern and may be disqualifying include:

a. involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;
b. association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
c. association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means;
d. involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

3. Conditions that could mitigate security concerns include:

a. the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
b. the individual's involvement was only with the lawful or humanitarian aspects of such an organization;
c. involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;
d. the person has had no recent proscribed involvement or association with such activities.

E. <u>CRIMINAL CONDUCT</u>.

1. A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

2. Conditions that could raise a security concern and may be disqualifying include:

a. any criminal conduct, regardless of whether the person was formally charged;
b. a single serious crime or multiple lesser offenses

3. Conditions that could mitigate security concerns include

a. the criminal behavior was not recent;
b. the crime was an isolated incident;
c. the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;
d. the person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;
e. there is clear evidence of successful rehabilitation.

F. <u>DRUG INVOLVEMENT</u>.

1. Improper or illegal involvement with drugs, raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

2. Drugs are defined as mood and behavior altering:

    a. drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens) and
    b. inhalants and other similar substances.
    c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

3. Conditions that could raise a security concern and may be disqualifying include:

    a. any drug abuse (see above definition);
    b. illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;
    c. failure to successfully complete a drug treatment program prescribed by a credentialed medical professional.
    d. Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination.

4. Conditions that could mitigate security concerns include:

    a. the drug involvement was not recent;
    b. the drug involvement was an isolated or infrequent event;
    c. a demonstrated intent not to abuse any drugs in the future;
    d. satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.

G. <u>EMOTIONAL, MENTAL AND PERSONALITY DISORDERS</u>.

1. Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability.

2. When appropriate, a credentialed mental health professional, acceptable to or approved by the government, should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated.

3. Conditions that could raise a security concern and may be disqualifying include:

    a. a diagnosis by a credentialed mental health professional that the individual has a disorder that could result in a defect in psychological, social, or occupational functioning;
    b. information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a diagnosed disorder, e.g. failure to take prescribed medication;
    c. a pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;
    d. information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

4. Conditions that could mitigate security concerns include:

    a. there is no indication of a current problem;
    b. recent diagnosis by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation;
    c. the past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

H. FINANCIAL CONSIDERATIONS.

1. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

2. Conditions that could raise a security concern and may be disqualifying include:

    a. a history of not meeting financial obligations;
    b. deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;
    c. inability or unwillingness to satisfy debts;
    d. unexplained affluence;
    e. financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

3. Conditions that could mitigate security concerns include:

a. the behavior was not recent;
b. it was an isolated incident;
c. the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);
d. the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
e. the affluence resulted from a legal source; and
f. the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

I. FOREIGN INFLUENCE.

1. A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are:

   a. not citizens of the United States or
   b. may be subject to duress.

2. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

3. Conditions that could raise a security concern and may be disqualifying include:

   a. an immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;
   b. sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;
   c. relatives, cohabitants, or associates who are connected with any foreign government;
   d. failing to report, where required, associations with foreign nationals;
   e. unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;
   f. conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;
   g. indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;
   h. a substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

4. Conditions that could mitigate security concerns include:

a. a determination that the immediate family member(s), cohabitant, or associate(s) in question would not constitute an unacceptable security risk;
b. contacts with foreign citizens are the result of official U.S. Government business;
c. contact and correspondence with foreign citizens are casual and infrequent;
d. the individual has promptly reported to proper authorities all contacts, requests, or threats from persons or organizations from a foreign country, as required;
e. foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

J. FOREIGN PREFERENCE.

1. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

2. Conditions that could raise a security concern and may be disqualifying include:

a. the exercise of dual citizenship;
b. possession and/or use of a foreign passport;
c. military service or a willingness to bear arms for a foreign country;
d. accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
e. residence in a foreign country to meet citizenship requirements;
f. using foreign citizenship to protect financial or business interests in another country;
g. seeking or holding political office in the foreign country;
h. voting in foreign elections; and
i. performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

3. Conditions that could mitigate security concerns include:

a. dual citizenship is based solely on parents' citizenship or birth in a foreign country;

b. indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
c. activity is sanctioned by the United States;
d. individual has expressed a willingness to renounce dual citizenship.

K. MISUSE OF INFORMATION TECHNOLOGY SYSTEMS.

1. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

2. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

3. Conditions that could raise a security concern and may be disqualifying include:

   a. illegal or unauthorized entry into any information technology system;
   b. illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;
   c. removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
   d. introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

4. Conditions that could mitigate security concerns include:

   a. the misuse was not recent or significant;
   b. the conduct was unintentional or inadvertent;
   c. the introduction or removal of media was authorized;
   d. the misuse was an isolated event;
   e. the misuse was followed immediately by a prompt, good faith effort to correct the situation.

L. OUTSIDE ACTIVITIES.

1. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

2. Conditions that could raise a security concern and may be disqualifying include:

    a. Any service, whether compensated, volunteer, or employment with:

        (1) a foreign country;
        (2) any foreign national;
        (3) a representative of any foreign interest;
        (4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

3. Conditions that could mitigate security concerns include:

    a. evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

    b. the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

M. <u>PERSONAL CONDUCT</u>.

1. Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

2. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

    a. refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

    b. refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

3. Conditions that could raise a security concern and may be disqualifying also include:

    a. reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

b. the deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
c. deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;
d. personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure;
e. a pattern of dishonesty or rule violations (see footnote);
f. association with persons involved in criminal activity.

4. Conditions that could mitigate security concerns include:

a. the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;
b. the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;
c. the individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;
d. omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;
e. the individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or pressure;
f. a refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;
g. association with persons involved in criminal activities has ceased.

N. SECURITY VIOLATIONS.

1. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

2. Conditions that could raise a security concern and may be disqualifying include:

a. unauthorized disclosure of classified information;
b. violations that are deliberate or multiple or due to negligence.

3. Conditions that could mitigate security concerns include actions that:

a. were inadvertent;
b. were isolated or infrequent;
c. were due to improper or inadequate training;
d. demonstrate a positive attitude towards the discharge of security responsibilities.

O. SEXUAL BEHAVIOR.

1. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to undue influence or coercion, or reflects lack of judgment or discretion. (see footnote) (Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance)

2. Conditions that could raise a security concern and may be disqualifying include:

   a. sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
   b. compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;
   c. sexual behavior that causes an individual to be vulnerable to undue influence or coercion;
   d. sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

3. Conditions that could mitigate security concerns include:

   a. the behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;
   b. the behavior was not recent and there is no evidence of subsequent conduct of a similar nature;
   c. there is no other evidence of questionable judgment, irresponsibility, or emotional instability;
   d. the behavior no longer serves as a basis for undue influence or coercion.

CHAPTER FIVE – DEPARTMENT OF ENERGY "Q" CLEARANCES

A. **General**. There are only a few positions/billets within the Coast Guard that are authorized access to Department of Energy (DOE) Restricted Data (Class Q) in connection with official duties. DOE Restricted Data relates to the design, manufacture and utilization of atomic/nuclear weapons; the production of special nuclear material or the use of nuclear material in the production of energy. DOE Restricted Data is assigned classification levels of Confidential, Secret or Top Secret, in keeping with the classification levels of other national defense information under provisions of E.O. 12958, National Security Information. Access to DOE Restricted Data is issued by the Department of Energy in accordance with the Atomic Energy Act of 1954 (Public Law 703, 83rd Congress).

B. **Responsibility.** Commandant (G-CFI) shall administer the DOE Nuclear Security (Class Q) clearance program within the Coast Guard, and is the final authority within the Coast Guard, regarding the issuance of DOE clearances for Coast Guard personnel.

C. **Submission of Request for DOE Clearances.** When a Coast Guard civilian employee or military member requires a DOE clearance, the responsible command must submit a written request, with sufficient justification, to Commandant (G-CFI). Upon approval of the request by the Chief of Coast Guard Security (G-CFI), the necessary investigation related forms and information will be forwarded to the civilian employee or military member, via the requesting command. Completed forms and information will be returned to Commandant (G.WKS-5) for review, approval and processing. The following forms and information shall be submitted:

1. SF 86, Questionnaire for Sensitive Positions, original and 2 copies;

2. DOE F 5631.18 Security Acknowledgment Statement;

3. SF 87, Fingerprint Card, 2 originals;

4. Information regarding any background investigations or derogatory information which the requesting office may have in its files regarding the individual; and

5. A letter of request, with specific justification for access to DOE Restricted Information, and the required forms and information listed above. Upon approval, Commandant (G-CFI) will forward the request and information to the Department of Energy for their adjudication and final determination.

D. **Unfavorable Cases.** Decisions by the Chief of Coast Guard Security (G-CFI) or DOE to grant or to deny Restricted Data Clearance or Access, are not subject to review or appeal by Coast Guard civilian employees or military members. Information obtained during the DOE clearance/access process may be utilized to make other security and suitability for employment determinations, as outlined in this manual.

E. **Notification of Clearance.** Commandant (G-CFI) will notify the civilian employee or military member, via his/her command, of the issuance of a DOE Restricted Data Clearance. The source document for the notification will be maintained by Commandant (G-CFI).

F. **Access Briefing .** The Command Security Officer or Command Classified Material Control Officer of the requesting Command will be responsible for providing a Q Clearance Security Briefing, through the utilization of briefing material provided by Commandant (G-CFI). The briefing official shall ensure that the person is thoroughly familiar with procedures required for safeguarding classified information and the special requirements relating to access to DOE Restricted Data. The briefing official shall also execute DOE Form 563 1. 18, Acknowledgment Statement, and return the form to Commandant (G-CFI), 2100 Second Street SW, Washington, DC 20593.

G. **Termination of Clearance.** Commands shall notify Commandant (G-CFI) when a DOE clearance/access is no longer required by the civilian employee or military member, because of duty changes, transfer or termination from employment or for any other reason. The employee or military member will be appropriately debriefed by the Command Security Officer or Classified Material Control Officer, who shall execute DOE Form F 5631.29, DOE Security Termination Statement, in duplicate. The Command will forward the DOE Security Termination Statement to Commandant (G-CFI), who will notify the Department of Energy that access is no longer required and request termination of the clearance. One copy of DOE Form F 5631.29 signed by the individual will be forwarded to DOE by Commandant (G-CFI), and one shall be retained by Commandant (G-CFI).

H. **Transfer of Clearance:** If an employee or military member transfers to the Coast Guard from another DOT administrations or from another Federal agency, and prior to the transfer was issued a DOE Q clearance and access to DOE Restricted Data, the command may request that the Q clearance and access authorization be transferred with the employee or military member to the Coast Guard. The command shall send their request to Commandant (G-CFI), with

name, social security number, and the DOE case file number (example: WA-123456), who will make a final determination for the Coast Guard, and if favorable, forward the request to DOE.

Investigative Standards for Background Investigations for Access to Classified Information

1. ***Introduction***. The following investigative standards are established for all United States Government Civilian and Military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

2. ***The Three Standards***. There are three standards (Table 1 in the Appendix summarizes when to use each one):

(a) The investigation and reinvestigation standards for "L" access authorizations and for access to CONFIDENTIAL and SECRET (including all SECRET-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by sect. 4.4 of Executive Order 12958);

(b) The investigation standard for "Q" access authorizations and for access to TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information; and

(c) The reinvestigation standard for continued access to the levels listed in para. 2(b).

3. ***Exception to Periods of Coverage***. Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the subject's eighteenth birthday to the present or to two years, which is longer.

4. ***Expanding Investigations***. Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

5. ***Transferability***. Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

6. Breaks in Service. If a person who requires access has been retired or separated from US government employment for less than two years and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (see Table 2).

7. ***The National Agency Check***. The National Agency Check is a part of all investigations and reinvestigations. It consists of a review of:

(a) Investigative and criminal history files of the FBI, including a technical fingerprint search;

(b) OPM's Security/Suitability Investigations Index; and

(c) DoD's Defense Clearance and Investigations Index; and

(d) such other national agencies (e.g., CIA, INS) as appropriate to the individual's background.

STANDARD A

National Agency Check with Local Agency Checks and

Credit Check (NACLC)

8. ***Applicability.*** Standard A applies to investigations and reinvestigations for:

(a) *Access to CONFIDENTIAL and SECRET* (including all SECRET-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by sect. 4.4 of Executive Order 12958), and

(b) "L" access authorizations.

9. ***For Reinvestigations***: When to Reinvestigate. The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation, including when there has been a break in service.)

10. ***Investigative Requirements***. Investigative requirements are as follows:

(a) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(b) *National Agency Check*: Completion of a National Agency Check.

(c) *Financial Review*: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

(d) *Date and Place of Birth*: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(e) *Local Agency Checks*: As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended

school within the last five years, and, if applicable, of the appropriate agency for any identified arrests.

11. ***Expanding the Investigation***. The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

STANDARD B

Single Scope Background Investigation (SSBI)

12. ***Applicability***. Standard B applies to initial investigations for:

(a) *Access to TOP SECRET* (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information; and

(b) *"Q" access authorizations*.

13. ***Investigative Requirements***. Investigative requirements are as follows:

(a) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(b) *National Agency Check*: Completion of a National Agency Check.

(c) *National Agency Check for the Spouse or Cohabitant* (if applicable): Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant.

(d) *Date and Place of Birth*: Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(e) *Citizenship*: For individuals born outside the United States, verification of US citizenship directly from the appropriate registration authority; verification of US citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

(f) *Education*: Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the subject during the most recent three years.

(g) *Employment*: Verification of all employments for the past seven years; personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military service, including discharge type. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

(h) *References*: Four references, of whom at least two are developed; to the extent practicable, all should have social knowledge of the subject and collectively span at least the last seven years.

(i) *Former Spouse*: An interview of any former spouse divorced within the last ten years.

(j) *Neighborhoods*: Confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

(k) *Financial Review*: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

(l) *Local Agency Checks*: A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (**NOTE:** If no residence, employment or education exceeds six months, local agency checks should be performed as deemed appropriate.)

(m) *Public Records*: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.

(n) *Subject Interview*: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

(0) *Polygraph* (only in agencies with approved personnel security polygraph programs): In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

14. ***Expanding the Investigation***. The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

STANDARD C

Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)

15. ***Applicability.*** Standard C applies to reinvestigations for:

(a) *Access to TOP SECRET* (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information; and

(b) *"Q" access authorizations*.

16. ***When to Reinvestigate***. The reinvestigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation (see Table 2).

17. ***Reinvestigative Requirements.*** Requirements are as follows:

(a) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(b) *National Agency Check*: Completion of a National Agency Check (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).

(c) National Agency Check for the Spouse or Cohabitant (if applicable): Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.

(d) *Employment:* Verification of all employment since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employment's of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

(e) *References*: Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practical, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

(f) *Neighborhoods:* Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Conformation of current residence regardless of length.

(g) *Financial Review*:

(1) *Financial Status*: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) *Check the Treasury's Financial Data Base*: Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

(h) *Local Agency Checks*: A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless

of duration. (NOTE: If no residence, employment or education exceeds six months, local agency checks should be performed as deemed appropriate.)

(i) *Former Spouse*: An interview with any former spouse unless the divorce took place before the data of the last investigation or reinvestigation.

(j) *Public Records*: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

(k) *Subject interview*: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements ands unsworn declarations may be taken whenever appropriate.

18. ***Expanding the Reinvestigation***. The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medial professionals, and law enforcement professionals may be conducted.

Investigative Standards for Temporary Eligibility for Access

1. ***Introduction***. The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, *Access to Classified Information*, are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

2. ***Temporary Eligibility for Access***. Based on a justified need meeting the requirements of sect. 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

3. ***Temporary Eligibility for Access at the CONFIDENTIAL and SECRET levels and Temporary Eligibility for "L" Access Authorization***. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).

4. ***Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization:*** *For Someone Who Is the Subject of a Favorable Investigation Not Meeting the Investigative Standards for Access at Those Levels*. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate

adjudicating authority, and expedited submission of a request for a Single Scope Background Investigation (SSBI).

5. ***Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization***: *For Someone Who Is Not the Subject of a Current, Favorable Personnel or Personnel-Security Investigation of Any Kind*. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited Single Scope Background Investigation (SSBI), and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

6. Additional Requirements by Agencies. Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968, Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, *Access to Classified Information.*

MILITARY PERSONNEL SECURITY PROGRAM
EVALUATION CHECK SHEET

A COMMENT IS REQUIRED IN THE COMMENTS SECTION FOR ALL ITEMS DEEMED "NOT APPLICABLE".

UNIT_____ DATE CONDUCTED:_____
COMMAND SECURITY OFFICER:_____
EVALUATOR:_____

	PAGE REF	YES	NO
Does command ensure a members need for security clearance/access is reviewed upon arrival?		____	____
Are personnel assigned to duries requiring access to classified information properly indoctrinated?		____	____
Are all personnel assigned to sensitive duties or access to classified information U.S. citizens?		____	____
Is U.S. citizenship verified prior to granting a final security clearance?		____	____
Are personnel selected to head delegations from the U.S. the subject of an SSBI?		____	____
Are Coast Guard representatives at international conferences the subject of an NAC?		____	____
Do commands conduct a self evaluation annually and submit copies to the cognizant security manager?		____	____
Are investigation requirements met for personnel requiring clearance?		____	____
Does the CSO review the monthly PMIS/JUMPS control report?		____	____
Does the CSO maintain a command roster of all personnel granted access to classified material?		____	____
Does the roster contain all of the required information?		____	____
When an individual requires clearance/access, does the command ensure that all conditions are met prior to utilizing a previous central adjudication facility (CAF) determination?		____	____

Is the appropriate entry made on a properly completed CG-5588 for re-approved clearances?	____ ____
Does the commanding officer sign the CG-5588 re-approving clearances for new personnel?	____ ____
Is the CG-5588 and other appropriate documents filed in the members PDR?	____ ____
Is the number of personnel granted access to classified information kept to an absolute minimum?	____ ____
If significant derogatory information is discovered on a cleared individual, is access suspended pending resolution?	____ ____
Does the command ensure that access is not granted solely to permit entry to or ease of movement within controlled areas?	____ ____
Does the command ensure that access is not granted merely as a result of any particular title, rank, position, or affiliation?	____ ____
Is access to classified information granted only to personnel for whom an appropriate investigation has been completed?	____ ____
Are proper procedures followed when granting an interim secret/confidential clearance?	____ ____
Are proper procedures followed when granting an interim top secret clearance?	_____ ____
Are interim clearances extended as necessary?	____ ____
Is the standard clearance notification letter sent when visiting other commands?	____ ____
Are NACLC requests reviewed by the CSO and submitted properly?	____ ____
Are SSBI requests justified, reviewed by the CSO for correctness and completeness and submitted to the cognizant security manager?	____ ____
When completing the SF-86 for an SSBI are the appropriate questions answered with a 10 year scope?	____ ____
Is a certificate of clearance and copy of an SF-312 filed in the PDR of members with a security clearance?	____ ____
Were all CG-5274's sent to CGPC for filing in the individuals permanent record?	____ ____

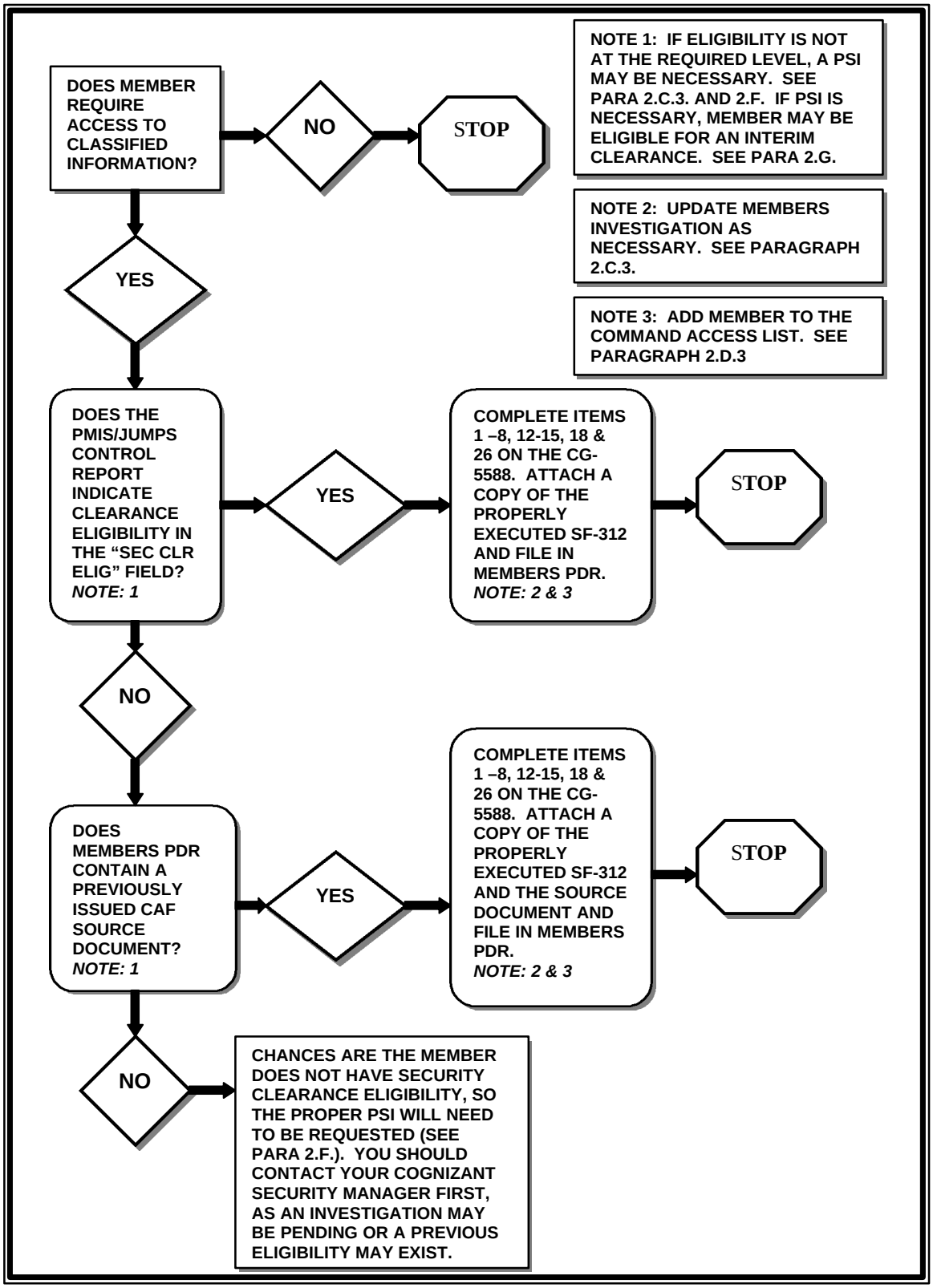
Does the command security officer notify the SSO if a letter of intent to deny or revoke clearance is received on an individual with SCI access?	____	____
Does the command ensure that individuals sign and forward acknowledgement portion of letters of intent when received?	____	____
Are individuals briefed on the effect of failure to appeal a security clearance determination?	____	____
Are the appropriate procedures followed when temporary access is granted?	____	____
Is derogatory information reported as part of the continuous evaluation program?	____	____
When a Coast Guard member marries or cohabits with a foreign born non-U.S. citizen is an SF-86 completed on the cohabitant as required?	____	____
Are all members of the command briefed from time to time on their responsibility in regards to classified and sensitive information?	____	____
Are all personnel reporting aboard the unit given an arrival briefing?	____	____
Are personnel who have access to classified information given an initial access briefing?	____	____
Have all personnel who have been granted access executed an SF-312 non-disclosure agreement?	____	____
Is the SF-312 properly accepted?	____	____
Are original SF-312's sent to Commandant (CGPC-ADM3) with a copy filed in the members PDR?	____	____
Are all personnel traveling to a foreign country given a foreign travel briefing?	____	____
Are all personnel who have access given an annual refresher brief?	____	____
Are personnel terminating government service given a final termination briefing?	____	____
Are briefings developed and documented correctly?	____	____
Are suicides and attempted suicides reported as required?	____	____
Are unauthorized absences reported as required?	____	____
Are Coast Guard personnel aware of techniques employed by foreign intelligence activities in attempting to obtain classified information?	____	____

Are individuals aware of their responsibilities when becoming aware of possible acts of sabotage, espionage or deliberate compromise of classified information?	____ ____

COMMENTS:_____
_____
_____
_____
_____

EVALUATOR
COMMENTS:_____
_____
_____
_____
_____

THIS EVALUATION CHECKLIST IS IN NO WAY INCLUSIVE OF ALL REQUIREMENTS CONTAINED WITHIN THE MANUAL..


DOES MEMBER REQUIRE ACCESS TO CLASSIFIED INFORMATION?
NO
STOP
YES
NOTE 1: IF ELIGIBILITY IS NOT AT THE REQUIRED LEVEL, A PSI MAY BE NECESSARY. SEE PARA 2.C.3. AND 2.F. IF PSI IS NECESSARY, MEMBER MAY BE ELIGIBLE FOR AN INTERIM CLEARANCE. SEE PARA 2.G.
NOTE 2: UPDATE MEMBERS INVESTIGATION AS NECESSARY. SEE PARAGRAPH 2.C.3.
NOTE 3: ADD MEMBER TO THE COMMAND ACCESS LIST. SEE PARAGRAPH 2.D.3
DOES THE PMIS/JUMPS CONTROL REPORT INDICATE CLEARANCE ELIGIBILITY IN THE "SEC CLR ELIG" FIELD? NOTE: 1
YES
COMPLETE ITEMS 1 –8, 12-15, 18 & 26 ON THE CG-5588. ATTACH A COPY OF THE PROPERLY EXECUTED SF-312 AND FILE IN MEMBERS PDR. NOTE: 2 & 3
STOP
NO
DOES MEMBERS PDR CONTAIN A PREVIOUSLY ISSUED CAF SOURCE DOCUMENT? NOTE: 1
YES
COMPLETE ITEMS 1 –8, 12-15, 18 & 26 ON THE CG-5588. ATTACH A COPY OF THE PROPERLY EXECUTED SF-312 AND THE SOURCE DOCUMENT AND FILE IN MEMBERS PDR. NOTE: 2 & 3
STOP
NO
CHANCES ARE THE MEMBER DOES NOT HAVE SECURITY CLEARANCE ELIGIBILITY, SO THE PROPER PSI WILL NEED TO BE REQUESTED (SEE PARA 2.F.). YOU SHOULD CONTACT YOUR COGNIZANT SECURITY MANAGER FIRST, AS AN INVESTIGATION MAY BE PENDING OR A PREVIOUS ELIGIBILITY MAY EXIST.